REMARKS

The Examiner has objected to Claims 4, 5, 20, 21, 36 and 37 for spelling errors. Applicant respectfully asserts that such objection has been overcome in view of the clarifications made to such claims.

The Examiner has rejected Claims 34-46 under 35 U.S.C. 112 for incorrect antecedent basis. Applicant has clarified such claims to overcome this rejection.

The Examiner has rejected Claims 1-46 under 35 U.S.C. 102(e) as being anticipated by Hypponen (International Publication No. WO02/19067). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to each of the independent claims.

With respect to each of the independent claims, the Examiner has relied on page 1, lines 29-31 to make a prior art showing of applicant's claimed "identifying code operable to identify one or more classes of malware threat against which said mobile computing device is to be protected" (see the same or similar, but not identical language in each of the independent claims).

Applicant notes that such excerpt only discloses a "number of different desktop anti-virus applications...which searches suspect files for the presence of predetermined virus signatures." Applicant respectfully asserts that generally disclosing applications that utilize virus signatures does not meet applicant's specifically claimed "one or more classes of malware threat" let alone identifying such classes for which "said mobile computing device is to be protected" (emphasis added), as claimed.

Still with respect to each of the independent claims, the Examiner has relied on item 9 in Figure 2 to make a prior art showing of applicant's claimed "generating code operable to generate from said master malware definition data said mobile computing

device malware definition data" (see the same or similar, but not identical language in each of the independent claims).

Applicant respectfully asserts that item 9 in Figure 2 is a database populated with known virus signatures where such database is part of the software architecture of the mobile device (see page 6, lines 2-3). Thus, Hypponen only teaches the virus database on the mobile device, and not mobile computing device malware definition data that is generated from said master malware definition data, as applicant claims.

In addition, the Examiner has relied on page 6, lines 21-30 to make a prior art showing of applicant's claimed "mobile computing device malware definition data identifying items of malware identified within said master malware definition data which are within classes of malware threat against which said mobile computing device is to be protected" (see the same or similar, but not identical language in each of the independent claims).

Applicant respectfully asserts that such excerpt only teaches a management agent on the mobile device that can access the virus signature database on the mobile device to enter new signatures, delete signatures or replace signatures. Again, such disclosure also fails to teach that the items identified are "within classes of malware threat against which said mobile computing device is to be protected" (emphasis added).

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the Hypponen reference, especially in view of the amendments made hereinabove. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has substantially incorporated the subject matter of Claims 2 and 7 et al. along with additional claim language into each of the independent claims.

With respect to the subject matter of Claim 2 et al., as presently incorporated into each of the independent claims, the Examiner has relied on Figure 3 to make a prior art showing of applicant's claimed technique "wherein said obtaining code, said identifying code and said generating code are executed by a fixed location computing device, said fixed location computer being operable to transfer to said mobile computing device one or more computer files including at least a computer file containing said mobile computer device malware definition data."

Applicant respectfully asserts that simply nowhere in Figure 3 is there any disclosure of "transfer to said mobile computing device one or more computer files including at least a computer file containing said mobile computer device malware definition data" (emphasis added). In fact, applicant notes that Figure 3 only shows a message related to a database update, but not a file that contains definition data, in the manner claimed by applicant.

With respect to the subject matter of Claim 7 et al., as presently incorporated into each of the independent claims, the Examiner has again relied on Figure 3 to make a prior art showing of applicant's claimed technique "wherein said fixed location computing device stores profile data identifying one or more different types of mobile computing device to which said fixed location computing device may transfer computer files and corresponding threat data identifying one or more classes of malware threat to which each of said mobile computing devices is vulnerable."

Applicant respectfully asserts that nowhere in Figure 3 is there even a suggestion of storing "profile data identifying one or more different types of mobile computing

device to which said fixed location computing device may transfer computer files," as claimed by applicant (emphasis added). Furthermore, Figure 3 also fails to teach storing "corresponding threat data identifying one or more classes of malware threat to which each of said mobile computing devices is vulnerable," as claimed by applicant (emphasis added).

Furthermore, applicant has incorporated the following claim language into each of the independent claims:

> "wherein only a subset of said master malware definition is used to generate said mobile computing device malware definition data for tailoring said mobile computing device malware definition data to accommodate only malware threats to which said mobile computing devices is vulnerable."

Applicant respectfully asserts that simply nowhere in Hypponen is there any disclosure of a subset of master malware definition, let alone where such subset is utilized for tailoring mobile computing device malware definition data to accommodate only malware threats to which said mobile computing devices is vulnerable.

Again, applicant respectfully asserts that the Hypponen reference does not anticipate applicant's specific claim language, since it fails to teach or suggest all of the claim limitations, as noted above. Applicant further notes that the prior art is also deficient with respect to the dependent claims.

Just by way of example, with respect to Claim 4 et al., the Examiner has relied on page 7, lines 16-19 to make a prior art showing of applicant's claimed technique "wherein, when said mobile computing device is connected to said fixed location computing device, different versions of user generated computer files respectively stored by said mobile computing device and said fixed location computing device are synchronized." Applicant respectfully asserts that such excerpt only teaches that "the management agent...[identifies] the missing updates and...request[s] these...from the

Management Centre 5." Clearly, simply identifying missing updates that have not been sent to the mobile device does not meet applicant's claimed "computer files respectively stored by said mobile computing device and said fixed location computing device [that] are synchronized" (emphasis added), as claimed.

With respect to the subject matter of Claim 10 et al., the Examiner has failed to make any specific prior art showing, in Hypponen, of applicant's claimed technique "wherein said fixed location computer device detects to which mobile computing devices it may transfer computer files by detecting installation upon said fixed location computing device of one or more transfer controlling computer programs operable to control transfer of computer files to one or more predetermined mobile computing devices."

Applicant respectfully asserts that nowhere in Hypponen is there any disclosure of a fixed location computer device detecting mobile computing devices, let alone mobile computing devices to which it may transfer computer files by detecting installation upon the fixed location computing device of one or more transfer controlling computer programs operable to control transfer of computer files to one or more predetermined mobile computing devices, in the manner specifically claimed by applicant.

Again, applicant respectfully asserts that the Hypponen reference does not anticipate applicant's specific claim language since it fails to teach or suggest all of the claim limitations, as noted above.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 47-48 below, which are added for full consideration:

> "wherein said fixed location device stores policy data including user defined settings identifying the manner in which said profile data is to be interpreted" (see Claim 47); and

"wherein said one or more classes of malware threat against which said mobile computing device is to be protected are chosen according to classes of malware threat known to pose a problem to said mobile computing device and classes for which it is desired to protect said mobile computing device according to user defined policies" (see Claim 48).

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P482/01.122.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100